UNITED STATES DISTRICT COURT
DISTRICT OF MARYLAND
GREENBELT DIVISION

CHRISTOPHER AMRINE, individually and on behalf of all others similarly situated, Plaintiff, v. J. J. F. MANAGEMENT SERVICES, INC. d/b/a FITZGERALD AUTO MALLS Defendant.	)	Case No.: **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Individually and on behalf of others similarly situated, Plaintiff Christopher Amrine brings this action against Defendant J.J.F. Management Services, Inc. d/b/a Fitzgerald Auto Malls. Plaintiff's allegations are based upon personal knowledge and acts, and upon information and belief as to all other matters based on the investigation conducted by and through Plaintiff's attorneys. Plaintiff believes that substantial additional evidentiary support for the allegations set forth herein exists and will be revealed after a reasonable opportunity for discovery.

I. INTRODUCTION

1. Every year millions of Americans have their valuable personal information stolen and sold online because of unauthorized data disclosures. Despite dire warnings about the severe impact of unauthorized data disclosures on Americans of all economic strata, companies still fail to put adequate security measures in place to prevent the unauthorized disclosure of private data.

2. Defendant Fitzgerald Auto Malls operates a series of auto dealerships with locations in Maryland, Pennsylvania, and Florida. As a part of that business, Defendant collect sensitive personal information from members of the public when they purchase automobiles.

3. This is a class action for damages against Defendant for their failure to exercise reasonable care in securing and safeguarding highly sensitive consumer data in connection with a large data breach impacting an unknown number of individuals' personal information[1] that occurred on or around February 4, 2024, (the "Data Breach") and impacted the highly sensitive data, including Plaintiff's and putative Class Members' (defined below), resulting in the unauthorized public release of highly sensitive information, including, but not limited to names and driver's license numbers (collectively, the "Private Information").

4. Fitzgerald Auto Malls collects information from customers and potential customers in the regular course of business operations.

5. To the world of cybercriminals, Fitzgerald Auto Malls' Private Information, including the data that was in possession at the time of the Data Breach, is extremely valuable. Stolen driver's licenses wreak financial havoc and identity theft issues for victims.

6. The security of Fitzgerald Auto Malls' Private Information is, therefore, of the utmost importance. Fitzgerald Auto Malls understood and appreciated the value of this Information by requesting it. yet chose to ignore the value of it by failing to invest in adequate data security measures that would protect Plaintiff and the Class from the unauthorized access to, and copying of, their Private Information.

7. Defendant failed to take necessary steps to protect the Private Information of customers.

---

[1] https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/31d2ab6d-85bd-42c7-b612-be4d4f891fff.html.

8. With their Private Information now in the hands of cybercriminals looking to profit from the theft, Plaintiff's and Class Members' Private Information is no longer secure, causing Plaintiff and Members of the Class to suffer (and continue to suffer) economic and non-economic harms, as well as a substantial and imminent risk of future economic and non-economic harms.

9. Fitzgerald Auto Malls understands the serious nature of data breaches and the potential theft and misuse of Fitzgerald Auto Malls' highly sensitive information resulting therefrom, and purports to address these issues. Fitzgerald Auto Malls acknowledges on its website that it "We restrict access to non-public personal information about you to our employees and affiliates employees who need to know that information to provide products or services to you. We maintain physical, electronic, and procedural safeguards that comply with federal regulations to guard your non-public personal information."[2]

10. Plaintiff and Class Members are no longer in possession of their Private Information, as it is no longer hidden but, instead, in the hands of cybercriminals who have already fraudulently misused such data.

11. While the exact reason(s) for the Data Breach remain unclear, there is no doubt that Defendant failed to adequately protect Plaintiff's and Class Members' Private Information and incorporate the tools necessary to keep such Private Information safe; such negligent failures resulted in the injuries alleged herein.

12. Had Plaintiff and the Class known that the Private Information they entrusted to Defendant in exchange for the goods offered would not be adequately protected, they would not have entrusted their valuable Private Information to Defendant in order to purchase goods and

[2] https://www.fitzmall.com/Legal/Privacy.

services.

13. Thus, on behalf of the Class of victims also impacted by the Data Breach described herein, Plaintiff seek, under state common law and consumer protection statutes, to redress Defendant's misconduct.

II. PARTIES

A. Plaintiff Christopher Amrine

14. Plaintiff Christopher Amrine has resided in Florida for the time period relevant to this Data Breach.

15. Mr. Amrine created an account with Fitzgerald Auto Malls around October of 2023, when he was looking to purchase a car.

16. Mr. Amrine provided his Private Information to the Defendant as a condition to shop for a car. He provided this information on the condition that it be maintained as confidential and with the understanding that Defendant would employ reasonable safeguards to protect his Private Information. If Mr. Amrine had known that Defendant would not adequately protect his Private Information, he would not have entrusted Defendant with his Private Information or allowed Defendant to maintain this sensitive Private Information.

17. In order to view his options for purchasing a car from Defendant, Plaintiff was required to provide his Private Information to Defendant.

18. At the time of the Data Breach, Fitzgerald Auto Malls retained Plaintiff Amrine's Private Information in its system.

19. Plaintiff Amrine is very careful about sharing his sensitive Private Information. Plaintiff stores any documents containing his Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the internet

or any other unsecured source.

20. Plaintiff Amrine became aware of the Data Breach through a notice sent via email dated April 25, 2025, notifying him that his name and driver's license or state issued identification number were potentially involved. On the same day he became aware of the Data Breach, Plaintiff immediately took steps to protect and vindicate his rights.

21. As a result of the Data Breach, Plaintiff Amrine made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching and verifying the legitimacy of the Data Breach as well as checking his financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff has spent significant time remedying the breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation.

22. Plaintiff Amrine suffered actual injury from having his Personal Information compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) loss of benefit of the bargain; (iii) lost time spent on activities remedying harms resulting from the Data Breach; (iv) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) diminution of value of his Private Information; and (vi) the continued and increased risk of fraud and identity theft.

23. In or around November 2024, Plaintiff Amrine received an alert from Experian notifying him that his email address was found on the dark web.

24. Plaintiff Amrine has suffered an increase in spam and fraudulent messaging since the Data Breach.

25. The Data Breach has caused Plaintiff Amrine to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant did not immediately notify him of the

incident.

26. As a result of the Data Breach, Plaintiff Amrine anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harm caused by the Data Breach. As a result of the Data Breach, Plaintiff Amrine is at present risk and will continue to be at increased risk of identity theft and fraud for years to come.

27. Plaintiff Amrine has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

B. Defendant J.J.F. Management Services, Inc. d/b/a Fitzgerald Auto Malls

28. Defendant J.J.F. Management Services, Inc. d/b/a Fitzgerald Auto Malls is a domestic profit corporation company organized under the laws of Maryland, with its principal place of business in Rockville, Maryland. Fitzgerald Auto Malls operates approximately twenty car dealership locations across Maryland, Pennsylvania, and Florida. Fitzgerald Auto Malls had access to users' Private Information and failed to secure the received Private Information or implement data security measures sufficient to ensure the sensitive customer data it stored would be securely handled.

III. JURISDICTION AND VENUE

29. Jurisdiction of this Court is founded upon 28 U.S.C. § 1332(d) because the matter in controversy exceeds the value of $5,000,000, exclusive of interests and costs, there are more than 100 class Members, and the matter is a class action in which any member of a class of Plaintiff is a citizen of a different state from any defendant.

30. This Court has personal jurisdiction over this action because Defendant is headquartered and has its primary place of business in Maryland and has thus availed itself of the

rights and benefits of the Maryland by engaging in activities including (i) directly and/or through their parent companies, affiliates and/or agents providing services throughout the United States and in this judicial district and abroad; (ii) conducting substantial business in this forum; (iii) having a registered agent to accept service of process in the State of Maryland; and/or (iv) engaging in other persistent courses of conduct and/or deriving substantial revenue from services provided in Maryland and in this judicial District.

31. Venue is proper in this District under 28 U.S.C. § 1391(b)(1) because Defendant resides within this District and has purposefully engaged in activities, including transacting business in this District and engaging in the acts and omissions alleged herein, in this District.

IV. FACTUAL ALLEGATIONS

A. The Data Breach

32. On or around Friday, April 25, 2025, Fitzgerald Auto Malls issued the following notice:

> The privacy and security of the personal information we maintain is of the utmost importance to us. We are writing to provide you with information regarding a cybersecurity incident that impacted and potentially involved your personal information. Please read this notice carefully, as it provides information about the incident and the significant measures we take to protect your information.
> *What Happened?*
> On or about February 4, 2024, Fitzgerald Auto Malls detected unauthorized access to our network as a result of a cybersecurity incident that resulted in the exposure of the data we maintain.
> *What We Are Doing.*
> Upon learning of the incident, we immediately took steps to secure our network and mitigate against any additional harm. We promptly launched an investigation assisted by external cybersecurity professionals experienced in handling these types of incidents. Our forensic investigation determined that data may have been accessed or acquired by the unauthorized party. We conducted a thorough manual review of the data potentially contained on the impacted servers. After extensive efforts to identify, review, and analyze the potentially impacted data, on March 28, 2025, we determined that the impacted files contained your personal information.

While cybersecurity threats continue to impact all of us, we are taking ever-increasing measures to protect the information entrusted to us. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information. In response to this incident and through our continuing comprehensive review, we have strengthened our network and implemented additional security improvements recommended by third-party cyber security experts.

What Information Was Involved?

The information that may have been accessed or acquired contained some of your personal information, including your name and drivers license or state issued identification number.

What You Can Do.

We have no evidence directly linking this incident to specific incidents of financial fraud or identity theft. However, we encourage impacted individuals to take actions to help protect their personal information. This letter also provides precautionary measures you can take to protect your personal information, including placing a Fraud Alert and Security Freeze on your credit files, and obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

For More Information.

If you have questions, please contact our dedicated and confidential call center at 1 833 998 5864. The response line is available for 90 days from the date of this letter, between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays.

We apologize for any inconvenience or concern this may cause. We have taken this matter very seriously and will continue to take significant measures to protect the personal information in our possession.

Sincerely,

Fitzgerald Auto Malls

33. Hackers were able to access sensitive Private Information of Fitzgerald Auto Malls' customers, including their names and driver's license numbers.

34. During the delay between the data breach in February of 2024 and notification in late April of 2025, the risks and damages to Plaintiff and Class Members were only increasing. A prompt and proper response from Defendant, including full disclosure to all Fitzgerald Auto Malls customers involved in the Data Breach of the extent of the Breach and the specific information impacted as a result of the Breach, as well as the risks users faced, would have mitigated those risks and resulting damages substantially, as users would have been able to

change their impacted drivers' information.

35. Thus, Defendant's disclosure, in addition to being unreasonably delayed, has been woefully inadequate and directly contributed to the damages suffered by Plaintiff and the Class thus far, and Defendant has yet to offer any remedy to assist Plaintiff and Class Members through the aftermath of its Breach.

36. Defendant not only failed to adequately disclose the Data Breach to impacted parties, but it also failed to explain the extent of the Data Breach, where the information was lost, and to whom it may have been lost.

B. Defendant Violated the FTC Act and Failed to Observe Reasonable and Adequate Data Security Measures

37. Defendant was prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 (the "FTC Act") from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g.*, *FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015).

38. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[3]

39. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cybersecurity guidelines for businesses.[4] The guidelines

---

[3] *Start With Security: A Guide for Business*, FED. TRADE. COMM'N (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf [hereinafter *Start with Security*].

[4] *Protecting Personal Information: A Guide for Business*, FED. TRADE. COMM'N (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf- 0136_proteting-personal-information.pdf.

note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

40. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[5]

41. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

42. Defendant was aware (or should have been aware), at all times, of the obligation to protect the Private Information of Plaintiff and Class Members because of its position as possessor and controller of such data. Defendant was also aware of the significant repercussions that would result from its failure to do so.

43. Plaintiff and Class Members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with their obligation to keep such information confidential and secure from unauthorized access.

44. Defendant did not follow industry standard security or data minimization policies.

---

[5] *Start with Security*, *supra* note 32.

45. Further, Defendant has been on notice for years that Plaintiff's and Class Members' Private Information was a target for malicious actors due to, among other reasons, the high value to these bad actors of the Private Information stored in Fitzgerald Auto Malls' system. Despite such knowledge, Defendant failed to implement and maintain reasonable and appropriate administrative and data security measures to protect Plaintiff's and Class Members' Private Information from unauthorized access that Defendant should have anticipated and guarded against.

46. Stolen driver's licenses can be used (alone or in combination with other information) by malicious actors to accomplish the following:

- Apply for credit cards
- Apply for financial loans (especially student loans)
- Open bank accounts
- Obtain or create fake driver's licenses
    - o Given to police for tickets
    - o Provided to accident victims
    - o Collect government unemployment benefits
    - o Create and sell underage fake IDs
- Replace/access account information on:
    - o LinkedIn
    - o Facebook/Meta
    - o WhatsApp
    - o Instagram
- Obtain a mobile phone

• Dispute or prove a SIM swap

• Redirect U.S. mail

• Apply for unemployment benefits

• Undocumented aliens may use them as a method to gain access to the U.S., and claim a lost or stolen passport

• Create a fake license as a baseline to obtain a Commercial Driver's License

• File tax returns or gain access to filed tax returns

• Engage in phishing and other social engineering scams

47. Almost half of data breaches globally are caused by internal errors relating to either human mismanagement of sensitive information or system errors.[6] Cybersecurity firm Proofpoint reports that since 2020, there has been an increase of internal threats through the misuse of security credentials or the negligent release of sensitive information.[7] To mitigate these threats, Proofpoint recommends that firms take the time to train their employees about the risks of such errors.[8]

48. As explained by the FBI, "[p]revention is the most effective defense against ransomware and it is critical to take precaution for protection."[9]

49. To prevent and detect unauthorized access to its system, Defendant could have, and should have, implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply the latest security updates

---

[6] COST OF A DATA BREACH REPORT, *supra* note 8, at 30.
[7] *The Human Factor 2021*, PROOFPOINT (July 27, 2021), https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-human-factor-report.pdf.
[8] *Id.*
[9] *See How to Protect Your Networks from RANSOMWARE*, FBI (2016) https ://www. fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view.

- Use threat and vulnerability management
- Perform regular audit; remove privilege credentials;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[10]

50. These are basic, common-sense security measures that every business, not only those who handle sensitive information, should be taking. Defendant, with the highly sensitive personal information in its possession and control, should be doing even more. By adequately taking these common-sense solutions, Defendant could have prevented this Data Breach from occurring.

51. Charged with handling sensitive Private Information, Defendant knew, or should have known, the importance of safeguarding the Private Information that was entrusted to them

[10] *See Human-operated ransomware attacks: A preventable disaster*, MICROSOFT (Mar. 5, 2020), https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-apreventable-disaster/.

and of the foreseeable consequences of a lapse in their data security. This includes the significant costs that would be imposed on Defendant's users because of a breach. Defendant failed, however, to take adequate administrative cybersecurity measures to prevent the Data Breach from occurring.

52. The Private Information was maintained in a condition vulnerable to misuse. The mechanism of the unauthorized access and the potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendant, and thus Defendant were on notice that failing to take reasonable steps necessary to secure the Private Information from those risks left the Private Information in a vulnerable position.

53. As evidenced by these failures by Defendant to comply with their legal obligations established by the FTC Act, as well as their failures to maintain the reasonable and adequate data security measures set forth herein, Defendant failed to properly safeguard Plaintiff's and Class Members' Private Information, allowing hackers to access and subsequently misuse it.

54. But for Defendant's unlawful conduct, hackers would not have accessed Plaintiff's and the putative Class Members' Private Information. Defendant's unlawful conduct has directly and proximately resulted in widespread attacks against Plaintiff and the Class.

55. National credit reporting company blogger, Sue Poremba, emphasized the value of driver's license to thieves and cautioned:

> If someone gets your driver's license number, it is also concerning because it's connected to your vehicle registration and insurance policies, as well as records on file with the Department of Motor Vehicles, place of employment (that keep copy of your driver's license on file), doctor's office, government agencies, and other entities. Having access to that one number can provide an identity thief with several pieces of information they want to know about you. Next to your Social Security number, your driver's license is one of the most important pieces to keep safe from thieves.

56. In fact, according to CPO Magazine, which specializes in news, insights, and resources for data protection, privacy, and cyber security professionals, "[t]o those unfamiliar with the world of fraud, driver's license numbers might seem like a relatively harmless piece of information to lose if it happens in isolation." Tim Sadler, CEO of email security firm Tessian, points out why this is not the case and why these numbers are very much sought after by cyber criminals:

> It's a gold mine for hackers. With a driver's license number, bad actors can manufacture fake IDs, slotting in the number for any form that requires ID verification, or use the information to craft curated social engineering phishing attacks. . . . bad actors may be using these driver's license numbers to fraudulently apply for unemployment benefits in someone else's name, a scam proving especially lucrative for hackers as unemployment numbers continue to soar. . . . In other cases, a scam using these driver's license numbers could look like an email that impersonates the DMV, requesting the person verify their driver's license number, car registration or insurance information, and then inserting a malicious link or attachment into the email.

57. Drivers' license numbers have been taken from auto–insurance providers by hackers in other circumstances, including Geico, Noblr, American Family, USAA, and Midvale all in 2021, indicating both that this specific form of PI is in high demand and also that Defendant knew or had reason to know that their security practices were of particular importance to safeguard consumer data.[11]

58. Plaintiff and Class Members Private Information is now in the hands of cybercriminals. This access has resulted in, at minimum, an invasion of Plaintiff's and Class Members' privacy and can lead to even greater damages.

---

[11] See United States Securities and Exchange Commission Form 8-K for INSU Acquisition Corp. II (Feb. 1, 2021), https://www.sec.gov/Archives/edgar/data/1819035/000121390021005784/ea134248-8k_insuacquis2.htm?=1819035-01022021 (accessed Apr. 27, 2021) (announcing a merger with auto-insurance company MetroMile, Inc., an auto-insurer, which announced a drivers' license number Data Disclosure on January 19, 2021); Ron Lieber, How Identity Thieves Took My Wife for a Ride, N.Y. TIMES (Apr. 27, 2021) (describing a scam involving drivers' license numbers and Progressive Insurance).

59. The actions described herein have resulted in emotional distress for Plaintiff and the Class. Plaintiff and the Class have lost all security and privacy over their driver's license number and other information.

60. Plaintiff and the Class are anxious and alert as they are at a substantial risk of being bombarded with phishing emails and other scams, in addition to the disclosure they have already suffered. Plaintiff is also suffering from the mental and emotional distress associated with such insecurity and uncertainty caused by the Data. In addition to financial loss, mental anguish, and risk of future harm, Class Members and Plaintiff continue to suffer from stress and anxiety as a result of the Data Breach.

61. As long as Plaintiff's and Class Members' Private Information is in the hands of cybercriminals, they will remain at substantial, imminent risk of continued misuse of their Private Information.

C. Damages to Plaintiff and the Class

62. Plaintiff has suffered damages from the Data Breach as set forth herein.

63. Defendant offered insufficient resolution, failing to even offer any kind of complimentary credit monitoring to victims.

64. If Defendant had disclosed the full extent of the Data Breach in February of 2024 instead of waiting over a year to do so, Plaintiff and Class Members would have been on heightened alert and changed their passwords, thus avoiding the thefts that ensued.

65. As to other forms of damages, Plaintiff's and Class Members' Private Information has been compromised and they have lost significant time having to sort through and change several accounts and passwords, and in addition, Plaintiff and Class Members have incurred the following types of damages: the lost value of their privacy; not receiving the benefit of their

bargain with Defendant; losing the difference in the value between the goods and services *with* adequate data security that Defendant promised and the goods and services actually received; the value of the lost time and effort required to mitigate the actual and potential impact of the Data Breach on their lives, including, *inter alia*, that required to change multiple account passwords, monitor accounts, and investigate how to maintain privacy from loss of driver's license information.

66. Additionally, Plaintiff and Class Members have been put at increased, substantial risk of future fraud and/or misuse of their Private Information, which may take years to manifest, discover, and detect, and may not occur until an attempt to purchase another insurance policy or vehicle.

67. Had Plaintiff been made aware of Defendant's lax data security practices, unwillingness to promptly and completely disclose data breaches such as this one, and failure to provide timely notice and mitigatory assistance, Plaintiff would not have agreed to allow his Private Information to be held by Defendant.

68. Defendant does not appear to be taking any measures to assist Plaintiff and Class Members. None of the recommendations described in the Data Breach Notification required Defendant to expend any effort to protect Plaintiff's and Class Members' Private Information.

D. The Monetary Value of Privacy Protections and Private Information

69. The fact that Plaintiff's and Class Members' Private Information was inadvertently disclosed to bad actors that should not have had access to it demonstrates the monetary value of the Private Information.

70. At all relevant times, Defendant understood the Private Information they collect from their users is highly sensitive and of significant property value.

71. An active and robust legitimate marketplace for PII exists. In 2019, the data brokering industry was worth roughly $200 billion. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to insurance companies.

72. As a result of the Data Breach, Plaintiff's and Class Members' Private Information, which has value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. This transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property.

V. CLASS ALLEGATIONS

73. Plaintiff brings this Action as a class action pursuant to Fed. R. Civ. P. 23 and seeks certification of the following nationwide Class (referred to herein as the "Class"):

> All persons whose personal information was accessed, compromised, copied, stolen, and/or exposed as a result of the Fitzgerald Auto Malls (and any of Fitzgerald Auto Malls' affiliates) Data Breach on or around February 4, 2024.

74. Excluded from the Class are Defendant, its officers and directors, and Members of their immediate families or their legal representatives, heirs, successors or assigns and any entity in which Defendant has or had a controlling interest.

75. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of the claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

76. **Numerosity—Federal Rule of Civil Procedure 23(a)(1).** The Members of the Class are so numerous that joinder of all Class Members would be impracticable. Upon information and belief, the Class numbers in the thousands. Moreover, the Class is composed of an easily ascertainable set of Fitzgerald Auto Malls customers who were thus impacted by the

Data Breach. The precise number of Class Members can be further confirmed through discovery, which includes Defendant's records. The disposition of Plaintiff's and Class Members' claims through a class action will benefit the parties and this Court.

77. **Commonality and Predominance—Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3).** Common questions of law and fact exist as to all Members of the Class and predominate over questions affecting only individual Members of the Class. Such common questions of law or fact include, *inter alia*:

- Whether Defendant's data security systems and/or protocol prior to and during the Data Breach complied with applicable data security laws and regulations;
- Whether Defendant's data security systems and/or protocol prior to and during the Data Breach were consistent with industry standards and best practices;
- Whether Defendant properly implemented their purported security measures to protect Plaintiff's and Class Members' Private Information from unauthorized capture, dissemination, and misuse;
- Whether Defendant took reasonable measures to determine the extent of the Data Breach after it first learned of same;
- Whether Defendant disclosed Plaintiff's and Class Members' Private Information in violation of the understanding that the Private Information was being disclosed in confidence and should be maintained;
- Whether Defendant willfully, recklessly, or negligently failed to maintain and execute reasonable procedures designed to prevent unauthorized access to Plaintiff's and the Class Members' Private Information;
- Whether Defendant were negligent in failing to properly secure and protect Plaintiff's and the Class's Private Information;
- Whether Defendant were unjustly enriched by their actions; and
- Whether Plaintiff and Class Members are entitled to damages, injunctive relief, or other equitable relief, and the measure of such damages and relief.

78. Defendant engaged in a common course of conduct giving rise to the legal rights

sought to be enforced by Plaintiff, on behalf of himself and other Members of the Class. Similar or identical common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that predominate in this action.

79. **Typicality—Federal Rule of Civil Procedure 23(a)(3).** Plaintiff's claims are typical of the claims of the other Members of the Class because, among other things, all Class Members were similarly injured and sustained similar monetary and economic injuries as a result of Defendant's uniform misconduct described herein and were thus all subject to the Data Breach alleged herein. Further, there are no defenses available to Defendant that are unique to Plaintiff.

80. **Adequacy of Representation—Federal Rule of Civil Procedure 23(a)(4).** Plaintiff are an adequate representative of the Class because their interests do not conflict with the interests of the Class they seek to represent, they retained counsel competent and experienced in complex class action litigation, and they will prosecute this action vigorously. The Class's interests will be fairly and adequately protected by Plaintiff and their counsel.

81. **Injunctive Relief—Federal Rule of Civil Procedure 23(b)(2).** Defendant acted and/or refused to act on grounds that apply generally to the Class, making injunctive and/or declaratory relief appropriate with respect to the Class under Fed. Civ. P. 23 (b)(2).

82. **Superiority—Federal Rule of Civil Procedure 23(b)(3).** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiff and the other Members of the Class are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendant, so it would be impracticable for Members of

the Class to individually seek redress for Defendant's wrongful conduct. Even if Members of the Class could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

83. Class certification is also appropriate under Rules 23(b)(1) and/or (b)(2) because:

- The prosecution of separate actions by the individual Members of the Class would create a risk of inconsistent or varying adjudications establishing incompatible standards of conduct for Defendant;
- The prosecution of separate actions by individual Class Members would create a risk of adjudication that would, as a practical matter, be dispositive of the interests of other Class Members not parties to the adjudications, or would substantially impair or impede their ability to protect their interests; and
- Defendant have acted and refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive relief with respect to the Members of the Class as a whole.

84. Class certification is also appropriate because this Court can designate particular claims or issues for class-wide treatment and may designate multiple subclasses pursuant to Fed. R. Civ. P. 23(c)(4).

85. No unusual difficulties are likely to be encountered in the management of this action as a class action.

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Class)

86. Plaintiff incorporate the preceding paragraphs as though fully set forth herein.

87. Upon Defendant's acceptance and storage of Plaintiff's and Class Members' Private Information in its system, Defendant undertook and owed a duty to Plaintiff and the Class to exercise reasonable care to secure and safeguard that Information and to use commercially reasonable methods to do so. Defendant knew that the Private Information was highly sensitive and confidential and should be protected as such.

88. Defendant owed a duty of care to provide security consistent with federal law and industry standards, to ensure their systems protected Class Members Private Information; and not to subject Plaintiff's and other Class Members' Private Information to an unreasonable risk of exposure and theft because Plaintiff and other Class Members were foreseeable and probable victims of any inadequate data security practices.

89. Plaintiff and Class Members entrusted Defendant with their Private Information. Defendant had an obligation to safeguard their information and was in a position to protect against the harm suffered by Plaintiff and Members of the Class as a result of the Data Breach.

90. Defendant owed numerous duties to Plaintiff and the Class, including the following:

- to exercise reasonable care in obtaining, retaining, securing, safeguarding, and protecting Private Information in its possession;
- to protect Private Information using reasonable and adequate security procedures and systems that are compliant with industry-standard practices; and
- to implement processes to quickly detect a data breach and to timely act on warnings about data breaches.

91. Defendant also breached their duty to Plaintiff and other Class Members to adequately protect and safeguard Private Information by disregarding standard information

security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured Private Information to unknown parties. Furthering its dilatory practices, Defendant failed to provide adequate supervision and oversight of the Private Information with which it was and is entrusted, in spite of the known risk and foreseeable likelihood of compromise and misuse, which permitted malicious bad actors to gather Plaintiff's and Class Members' Private Information and intentionally disclose it to others and/or misuse it without consent, resulting in the harms alleged herein.

92. Defendant knew, or should have known, of the risks inherent in collecting and storing Plaintiff's and Class Members' Private Information and the importance of adequate data security.

93. Defendant knew, or should have known, that its data systems and privacy protocols and procedures would not adequately safeguard Plaintiff's and Class Members' Private Information.

94. Defendant breached its duties to Plaintiff and Class Members by failing to provide fair, reasonable, or adequate computer systems, networks, and/or data security practices to safeguard Plaintiff's and Class Members' Private Information.

95. Because Defendant knew that the theft of the highly sensitive data stored in its systems would damage millions of individuals and businesses, including Plaintiff and Class Members, Defendant had a duty to implement sufficient privacy practices and procedures and adequately protect its data systems and the Private Information contained therein.

96. Defendant's duty of care to use reasonable data security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and Class Members, which is recognized by laws and regulations, including but not limited to, common law.

Defendant were in a position to ensure that its systems and protocols were sufficient to protect against the foreseeable risk of harm to Class Members from the compromise of the data with which it was entrusted.

97. In addition, Defendant had a duty to employ reasonable data security measures under Section 5 of the FTC Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable data security measures to protect confidential data.

98. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described herein, but also because Defendant were bound by industry standards to do more to protect the confidential data that was compromised as a result of the Data Breach.

99. Defendant's own conduct also created a foreseeable risk of harm to Plaintiff and Class Members and their Private Information. Defendant's misconduct included failing to (1) secure Plaintiff's and Class Members' Private Information; (2) comply with industry standard security practices; (3) implement adequate system and event monitoring; and (4) implement the systems, policies, and procedures necessary to prevent the Data Breach.

100. Defendant breached its duties, and thus were negligent, by failing to use reasonable measures to protect Class Members' Private Information, and by failing to provide timely notice of the Data Breach. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

- Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;
- Failing to adequately monitor the security of its networks and systems;

- Allowing unauthorized access to Class Members' Private Information;
- Encouraging exposure of Class Members' Private Information by cross-referencing with third-parties as a business model;
- Failing to detect in a timely manner that Class Members' Private Information had been compromised; and
- Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for fraud and other damages.

101. Through Defendant's acts and omissions described in this Complaint, including its failure to provide adequate data security and protect Plaintiff's and Class Members' Private Information from being foreseeably accessed, stolen, disseminated, and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure Plaintiff's and Class Members' Private Information during the time it was within Defendant's possession and control.

102. Defendant's conduct was grossly negligent and departed from all reasonable standards of care, including, but not limited to, failing to adequately protect the Private Information, and failing to provide Plaintiff and Class Members with timely notice that their sensitive Private Information had been compromised.

103. Neither Plaintiff nor Class Members contributed to the Data Breach and subsequent misuse of their Private Information as described in this Complaint. Any and all actions taken by Plaintiff and Class Members which Defendant may argue contributed to the misuse of the compromised Private Information were reasonable under the circumstances.

104. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members suffered damages as alleged herein.

105. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; and (ii) submit to future bi-annual audits of those systems and monitoring procedures.

COUNT II
BREACH OF CONTRACT/BREACH OF IMPLIED COVENANT OF GOOD FAITH AND FAIR DEALING
(On Behalf of Plaintiff and the Class)

106. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

107. Plaintiff and Class Members entered into valid and enforceable express contracts with Defendant under which Plaintiff and Class Members agreed to provide their Private Information to Defendant, and Defendant agreed to provide confidential services that included the implementation of adequate data security standards, protocols, and procedures to ensure the protection of Plaintiff's and Class Members' Private Information.

108. In every contract entered into between Plaintiff and Class Members and Defendant, including those at issue here, there is an implied covenant of good faith and fair dealing obligating the parties to refrain from unfairly interfering with the rights of the other party or parties to receive the benefits of the contracts. This covenant of good faith and fair dealing is applicable here as Defendant was obligated to protect (and not interfere with) the privacy and protection of Plaintiff's and Class Members' Private Information.

109. To the extent Defendant's obligation to protect Plaintiff's and Class Members' Private Information was not explicit in those express contracts, the contracts also included implied terms requiring Defendant to implement data security adequate to safeguard and protect the confidentiality of Plaintiff's and Class Members' Private Information, including in accordance with trade regulations, federal, state and local laws, and industry standards. No

customer would have entered into these contracts with Defendant without the understanding that their Private Information would be safeguarded and protected; stated otherwise, data security was an essential term of the parties' contracts.

110. Plaintiff and Class Members agreed, among other things, to provide their Private Information in exchange for Defendant's services.

111. The protection of Plaintiff's and Class Members' Private Information is a material aspect of Plaintiff's and Class Members' contracts with Defendant.

112. Defendant's promises and representations described above relating to industry standards and Defendant's purported concern about its users' privacy rights are express terms of the contracts between Defendant, including Plaintiff and Class Members. Defendant breached these promises by failing to comply with reasonable industry practices.

113. Plaintiff and Class Members read, reviewed, and/or relied on statements made by or provided by Defendant and/or otherwise understood that Defendant would protect its Fitzgerald Auto Malls' Private Information if that information were provided to Defendant.

114. Plaintiff and Class Members fully performed their obligations under their contracts with Defendant; however, Defendant did not.

115. As a result of Defendant's breach of these terms, Plaintiff and Class Members have suffered a variety of damages including but not limited to: the lost value of their privacy; not receiving the benefit of their bargain with Defendant; losing the difference in the value between the services *with* adequate data security that Defendant promised and the services actually received; the value of the lost time and effort required to mitigate the actual and potential impact of the Data Breach on their lives, including, inter alia, that required to change multiple account passwords, monitor accounts, and investigating how to protect themselves.

Additionally, Plaintiff and Class Members have been put at increased risk of future fraud and/or misuse of their Private Information, which may take years to manifest, discover, and detect.

116. Plaintiff and Class Members are therefore entitled to damages, including restitution and unjust enrichment, disgorgement, declaratory and injunctive relief, and attorney fees, costs, and expenses.

COUNT III
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class)

117. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

118. Plaintiff brings this claim alternatively to his claim for breach of contract.

119. Through its course of conduct, Defendant entered into implied contracts with Plaintiff and Class Members for the provision of password and identity management services, as well as implied contracts for Defendant to implement data security practices adequate to safeguard and protect the privacy of Plaintiff's and Class Members' Private Information.

120. Specifically, Plaintiff entered into valid and enforceable implied contracts with Defendant when they first began using Defendant's services.

121. The valid and enforceable implied contracts to provide confidential services that Plaintiff and Class Members entered into with Defendant include Defendant's promise to protect nonpublic Private Information entrusted to it.

122. When Plaintiff and Class Members provided their Private Information to Defendant in exchange for Defendant's services, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

123. Defendant solicited and invited Plaintiff and Class Members to provide their

Private Information as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offer and provided their Private Information to Defendant.

124. By entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

125. Under these implied contracts, Defendant promised and were obligated to: (a) protect Class Members drivers' license and vehicle information (b) provide services inclusive of protecting Private Information to Plaintiff's and Class Members; and (c) protect Plaintiff's and the Class Members' Private Information provided to obtain such benefits of such services. In exchange, Plaintiff and Members of the Class agreed to turn over their Private Information to Defendant.

126. Both the provision of services and the protection of Plaintiff's and Class Members' Private Information were material aspects of these implied contracts.

127. The implied contracts for the provision of services, including but not limited to, the maintenance of the privacy of Plaintiff's and Class Members' Private Information, are also acknowledged, memorialized, and embodied in Defendant's Terms of Service for personal users.

128. Defendant's express representations, including, but not limited to, the express representations found in its Terms of Service, memorialize and embody the implied contractual obligations requiring Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff and Class Members, and to protect the privacy of Plaintiff's and Class Members' Private Information.

129. Customers of auto dealerships value their privacy and the ability to keep their Private Information associated with obtaining such services. Plaintiff and Class Members would

not have entrusted their Private Information to Defendant and entered into these implied contracts with Defendant without an understanding that their Private Information would be safeguarded and protected; nor would they have entrusted their Private Information to Defendant in the absence of the implied promise by Defendant to monitor the Private Information and to ensure that it adopted reasonable administrative and data security measures.

130. Plaintiff and Class Members agreed and provided their Private Information to Defendant in exchange for, among other things, the protection of their Private Information.

131. Plaintiff and Class Members performed their obligations under the contract when they made payment and turned over their Private Information to Defendant.

132. Defendant materially breached its contractual obligation to protect the nonpublic Private Information it gathered when the Private Information was compromised and subsequently misused as a result of the Data Breach.

133. Defendant materially breached the terms of these implied contracts, including, but not limited to, the terms stated in the relevant Privacy Policy. Defendant did not maintain the privacy of Plaintiff's and Class Members' Private Information as evidenced by its recent notices of the Data Breach posted on its blog. Specifically, Defendant did not comply with industry standards, standards of conduct embodied in statutes like Section 5 of the FTCA, or otherwise protect Plaintiff's and Class Members' Private Information as set forth above.

134. The Data Breach was a reasonably foreseeable consequence of Defendant's data security failures in breach of these contracts.

135. As a result of Defendant's failure to fulfill the data security protections promised in these contracts, Plaintiff and Class Members did not receive the full benefit of their bargain with Defendant, and instead received goods and services that were of a diminished value to that

described in the contracts. Plaintiff and Class Members therefore were damaged in an amount at least equal to the difference in the value of the insurance accounts *with* data security protection that Defendant agreed to provide and the services Defendant actually provided.

136. Had Defendant disclosed their administrative and data security measures were inadequate or that it did not adhere to industry-standard security measures, neither Plaintiff, Class Members, nor any reasonable person would have utilized services from Defendant.

137. As a direct and proximate result of the Data Breach, Plaintiff and Class Members have been harmed and suffered, and will continue to suffer, actual damages and injuries, including without limitation, the release and disclosure of their Private Information, the loss of control of their Private Information, the imminent risk of suffering additional damages in the future, out of pocket expenses, and the loss of the benefit of the bargain they struck with Defendant.

138. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

139. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.,* strengthen their data security systems and monitoring procedures, and immediately take on the burden of long-term, adequate credit monitoring to all Class Members.

COUNT IV
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

140. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

141. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they provided Defendant with their Private Information. In exchange, Plaintiff and

Class Members should have received from Defendant the services that were the subject of the transaction and were entitled to have Defendant protect their Private Information with adequate data security.

142. Defendant knew and appreciated that Plaintiff and Class Members conferred a benefit on them and accepted and retained that benefit. Defendant profited from Plaintiff's and Class Members' providing their Private Information for Defendant's business purposes.

143. Defendant failed to secure Plaintiff's and Class Members' Private Information and, therefore, did not provide full compensation for the benefit that Plaintiff's and Class Members' Private Information provided.

144. Defendant acquired the Private Information through inequitable means as it failed to disclose the inadequate security practices alleged herein.

145. If Plaintiff and Class Members knew that Defendant did not have data security safeguards in place that were adequate to secure their Private Information from unauthorized access, they would not have used Defendant's services.

146. Under the circumstances, it would be unjust for Defendant to be permitted to retain any of the benefits that Plaintiff and Class Members conferred upon it.

147. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds in the amount of the benefits that it unjustly received from them by way of possessing and controlling Plaintiff's and Class Members' Private Information.

148. This claim is being asserted in the alternative to Plaintiff's claims for breach of contract.

COUNT V
BREACH OF FIDUCIARY DUTY

(On Behalf of Plaintiff and the Class)

149. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

150. Plaintiff and Class Members have an interest, both equitable and legal, in the Private Information that was conveyed to and collected, stored, and maintained by Defendant and which was ultimately compromised by unauthorized cybercriminals as a result of the Data Breach.

151. Defendant, in taking possession of this highly sensitive information, have a special relationship with Plaintiff and the Class. As a result of that special relationship, Defendant were provided with and stored private and valuable information belonging to Plaintiff and the Class, which Defendant were required by law and industry standards to maintain in confidence.

152. In light of the special relationship between Defendant and Plaintiff and Class Members, whereby Defendant became a guardian of Plaintiff's and Class Members' Private Information, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for the benefit of its customers, including Plaintiff and Class Members, for the safeguarding of Plaintiff's and Class Members' Private Information.

153. Defendant had a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of this relationship, in particular, to keep secure Plaintiff's and Class Members' Private Information and to maintain the confidentiality of their Private Information.

154. Defendant owed a duty to Plaintiff's and Class Members to exercise the utmost care in obtaining, retaining, securing, safeguarding, deleting, and protecting their Private

Information in its possession from being compromised, lost, stolen, accessed by, misused by, or disclosed to unauthorized persons.

155. Plaintiff and Class Members have a privacy interest in their personal and proprietary matters and Defendant had a duty not to disclose such confidential information.

156. Plaintiff's and Class Members' Private Information is not generally known to the public and is confidential by nature. Moreover, Plaintiff and Class Members did not consent to nor authorize Defendant to release or disclose their Private Information to unknown criminal actors.

157. Defendant breached its fiduciary duty to Plaintiff's and Class Members when Plaintiff's and Class Members' Private Information was disclosed to unknown criminal hackers by way of Defendant's own acts and omissions, as alleged herein.

158. Defendant knowingly breached its fiduciary duties by failing to safeguard Plaintiff's and Class Members' Private Information, including by, among other things: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of the Private Information; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the Breach at the time it began or within a reasonable time thereafter and give adequate notice to Plaintiff and Class Members thereof; (g) failing to follow its own privacy policies and practices published online; (h) storing Private Information in an

unencrypted and vulnerable manner, allowing its disclosure to hackers; and (i) making an unauthorized and unjustified disclosure and release of Plaintiff's and Class Members' Private Information to a criminal third party.

159. But for Defendant's wrongful breach of its fiduciary duties owed to Plaintiff and Class Members, their privacy would not have been compromised and their Private Information would not have been accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by and/or viewed by unauthorized third parties.

160. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiff and Class Members have suffered or will suffer injuries, including but not limited to, the following: loss of their privacy and confidentiality of their Private Information; theft of their Private Information; costs associated with the detection and prevention of fraud and unauthorized use of their Private Information; costs associated with purchasing credit monitoring and identity theft protection services; loss of time and costs associated with investigating purchase of vehicle or insurance; costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Defendant's Data Breach – including finding fraudulent charges, enrolling in credit monitoring and identity theft protection services, and filing reports with the police and FBI; the imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their Private Information being placed in the hands of criminals; damages to and diminution in value of their Private Information entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiff's and Class Members' data against theft and not allow access and misuse of their data by others; continued risk of exposure to hackers and thieves of their Private Information, which remains in

Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' data; and/or mental anguish accompanying the loss of confidence and disclosure of their Private Information.

161. Defendant breached their fiduciary duty to Plaintiff's and Class Members when they made an unauthorized release and disclosure of their confidential Private Information and, accordingly, it would be inequitable for Defendant to retain the benefits they have received at Plaintiff's and Class Members' expense.

162. Plaintiff and Class Members are entitled to damages and/or disgorgement or restitution, in an amount to be proven at trial.

COUNT VI
DECLARATORY JUDGMENT AND INJUNCTIVE RELIEF
(On Behalf of Plaintiff and the Class)

163. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

164. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. The Court also has broad authority to restrain acts, such as here, that are tortious and violate the terms of the regulations described in this Complaint.

165. An actual controversy has arisen in the wake of the Data Breach regarding Defendant's present and prospective duties to reasonably safeguard users' Private Information and whether Defendant are maintaining data security measures adequate to protect the Class Members, including Plaintiff, from further data breaches that compromise their Private Information, including but not limited to, their respective customer accounts.

166. Plaintiff alleges that Defendant's data-security measures remain inadequate. In

addition, Plaintiff and the Class continue to suffer injury as a result of the compromise of their Private Information and remain at imminent risk that further compromises of their Private Information and continued fraudulent activity against them will occur in the future.

167. Pursuant to its authority under the Declaratory Judgment Act, Plaintiff asks the Court to enter a judgment declaring, among other things, the following: (i) Defendant owe a duty to secure consumers' Private Information and to timely notify consumers of a data breach under the common law, the DDPA, and Section 5 of the FTC Act; and (ii) Defendant are in breach of these legal duties by failing to employ reasonable measures to secure consumers' Private Information in their possession and control.

168. Plaintiff further asks the Court to issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with law and industry standards to protect consumers' Private Information from future data breaches.

169. If an injunction is not issued, the Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Fitzgerald Auto Malls. The risk of another such breach is real, immediate, and substantial. If another breach at Fitzgerald Auto Malls occurs, the Class Members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and Class Members will be forced to bring multiple lawsuits to rectify the same misconduct.

170. The hardship to the Class Members if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Among other things, if a similar data breach occurs again due to the repeated misconduct of Defendant, the Class Members will likely be subjected to substantial hacking and phishing attempts and other damage, in addition to the damages already suffered. On the other hand, the cost to Defendant of complying with an

injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant have pre-existing legal obligations to employ such measures.

171. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing additional data breaches at Fitzgerald Auto Malls, thus eliminating the additional injuries that would result to the Class Members and the millions of consumers whose personal and confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Class proposed in this Complaint, respectfully requests that the Court enter judgment in favor of Plaintiff and the Class and against Defendant, as follows:

A. For an Order certifying this action as a class action and appointing Plaintiff and their counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to Defendant's lax data security practices, procedures, networks, and systems that led to the unauthorized disclosure and subsequent misuse of Plaintiff's and Class Members' Private Information, and from failing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

C. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity all types of Private Information compromised during the Data Breach;

D. For equitable relief requiring restitution and disgorgement of the benefits wrongfully retained by Defendant as a result of its wrongful conduct;

E. For an award of damages, compensatory damages and/or restitution or disgorgement, in an amount to be determined, as allowable by law;

F. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

G. Pre- and post-judgment interest on any amounts awarded; and

H. Such other and further relief as this court may deem just and proper.

JURY DEMAND

Plaintiff demands a trial by jury on all issues so triable.

Date: April 30, 2025

Respectfully Submitted,

/s/ *Nicholas A. Migliaccio*

Nicholas A. Migliaccio
Jason S. Rathod
MIGLIACCIO & RATHOD, LLP
412 H Street, NE, Suite 302
Washington, DC 20002
Phone: 202-470-520
Fax: 202-800-2730
nmigliaccio@classlawdc.com
jrathod@classlawdc.com

Counsel for Plaintiff and the Putative Class

*To apply for admission *pro hac vice*